Seminar:

Solutions and Infrastructure to ensure Trust in E-Commerce

Marco Casassa Mont
marco_casassa-mont@hp.com

Trusted E-Services Laboratory
Hewlett-Packard Laboratories,
Bristol, UK
www.hpl.hp.com

Presentation Outline

1. Overview of Concepts and basic Infrastructure:

- ***Access Control***
- ***PKI & Trust***
- ***Policy and Policy Management***

2. Solutions and Infrastructure to underpin Trust in E-Commerce:

- ***PASTELS (HPL Bristol): Trust & Authorization Management in B2B***

3. Moving Towards the Future

- ***Trust Services eco-system … creating a Safety Net for E-Commerce***

Terminology

- **Access Control: controllo di accesso**
- **Role: ruolo**
- **Authorization: autorizzazione**
- **Authentication: identificazione**
- **Policy: politiche, regole, condizioni**
- **PKI: Public key Infrastructure (infrastr. di crittografia pubblica)**
- **Trust: fiducia, …**

PART 1

Overview of Concepts and Basic Infrastructure

Access Control Overview

Access Control

- **Defines what a user can do on a resource**
- **Limits the operations that a user of a system can do**
- **It is enforced by a Reference Monitor which mediates every attempted access by a user to objects in the system**

Access Control Lists

	Resource 1	Resource 2	Resource 3		Resource K
User 1			R, W, E		
User 2			R, W		
User 3			R		
User n			E		

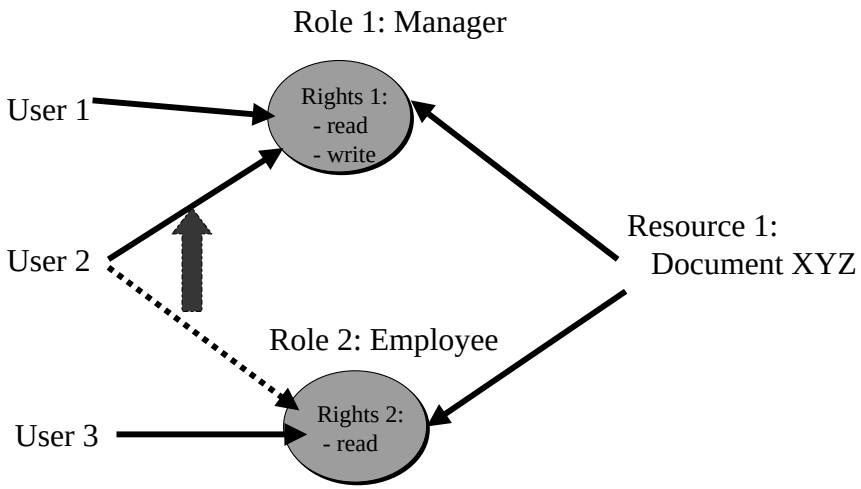
Access Control List

- **Complexity in administering large number of users**

Role Based Access Control (RBAC)

- **Role (General) : set of actions and responsabilities associated with a particular activity**
- **Definition of Roles in the system (administrator, engineer, project manager, etc.)**
- **Role: contains authorizations on objects**
- **Users are assigned to roles**
- **Simple RBAC model = Group-based ACL (Windows NT access control, …)**

Role Based Access Control (RBAC)

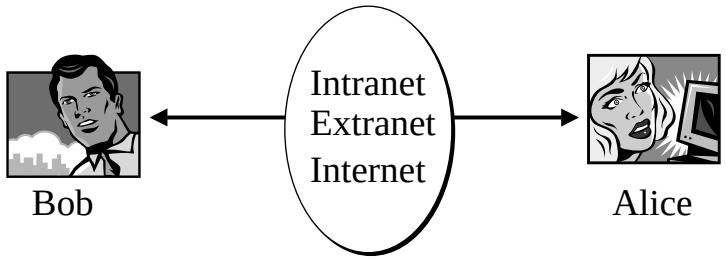


Public Key Infrastructure (PKI) and Trust

Outline

- **Basic Problem: Confidence and Trust**
- **Background: Cryptography, Digital Signature, Digital Certificates**
- **(X509) Public Key Infrastructure (PKI)**

Basic Problem

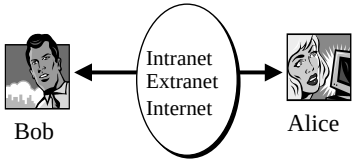


Bob and Alice want to exchange data in a digital world.

There are Confidence and Trust Issues …

Confidence and Trust Issues

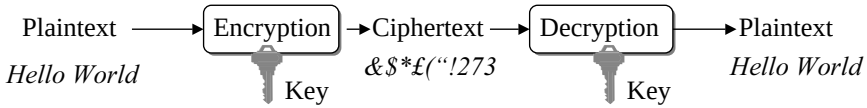
- **In the Identity of an Individual or Application**
  AUTHENTICATION
- **That the information will be kept Private**
  CONFIDENTIALITY
- **That information cannot be Manipulated**
  INTEGRITY
- **That information cannot be Disowned**
  NON-REPUDIATION



Starting Point: Cryptography

Cryptography

It is the science of making the cost of acquiring or altering data greater than the potential value gained



Cryptographic Algorithms

All cryptosystems are based only on three Cryptographic Algorithms:

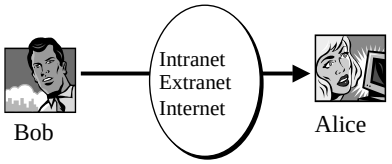
- MESSAGE DIGEST *(MD2-4-5, SHA, SHA-1, ...)*
  Maps variable length plaintext into fixed length ciphertext
  No key usage, computationally infeasible to recover the plaintext

- SECRET KEY *(Blowfish, DES, IDEA, RC2-4-5, Triple-DES, ...)*
  Encrypt and decrypt messages by using the same Secret Key

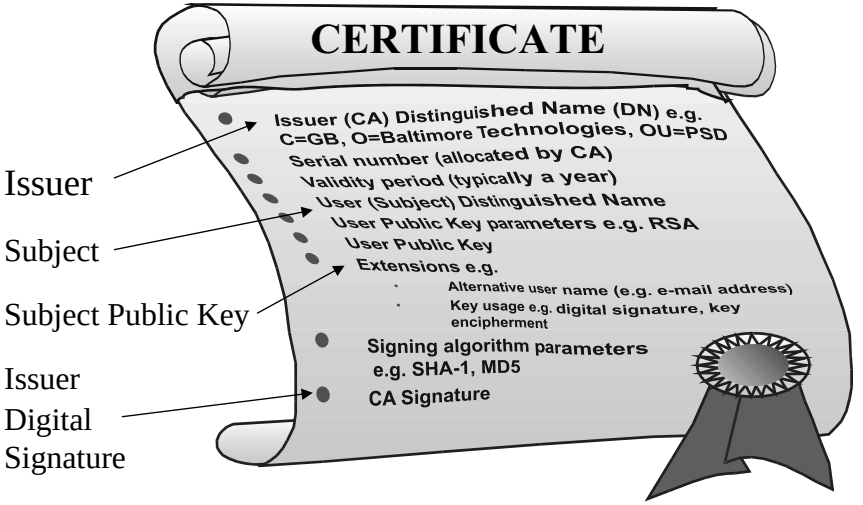
- PUBLIC KEY *(DSA, RSA, ...)*
  Encrypt and decrypt messages by using two different Keys: Public Key, Private Key (coupled together)

Digital Signature

A Digital Signature is a data item that vouches the origin and the integrity of a Message



Digital Identity Certificate



Digital Certificate

Problems

- How are Digital Certificates Issued?
- Who is issuing them?
- Why should I Trust the Certificate Issuer?
- How can I check if a Certificate is valid?
- How can I revoke a Certificate?
- Who is revoking Certificates?

Moving towards PKI ...

Public Key Infrastructure (PKI)

- A Public Key Infrastructure is an Infrastructure to support and manage Public Key-based Digital Certificates

- Potentially it is a complex distributed Infrastructure over the Internet

Public Key Infrastructure (PKI)

Focus on:

- X509 PKI
- X509 Digital Certificates

➔ Standards defined by IETF, PKIX WG:
http://www.ietf.org/

... even if X509 is not the only approach (e.g. SPKI)

X509 PKI – Technical View

Basic Components:

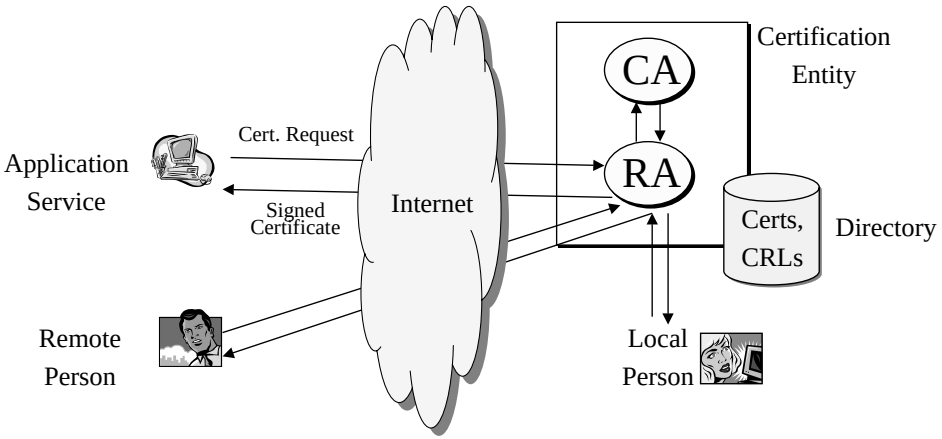
- Certificate Authority (CA)
- Registration Authority (RA)
- Certificate Distribution System

"Provider" Side

- PKI enabled applications

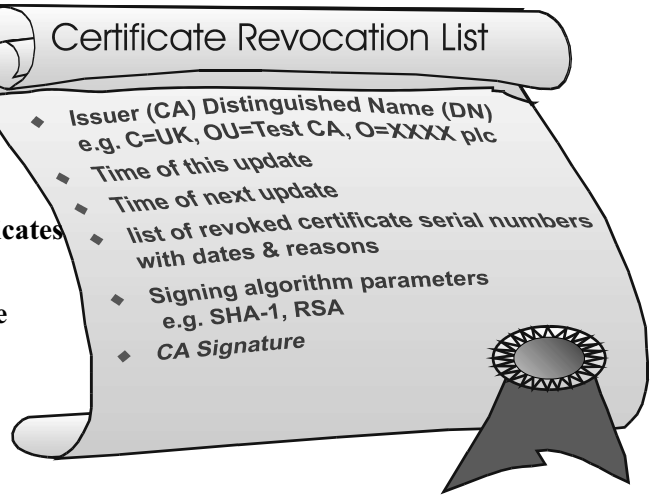
"Consumer" Side

X509 PKI – Simple Model

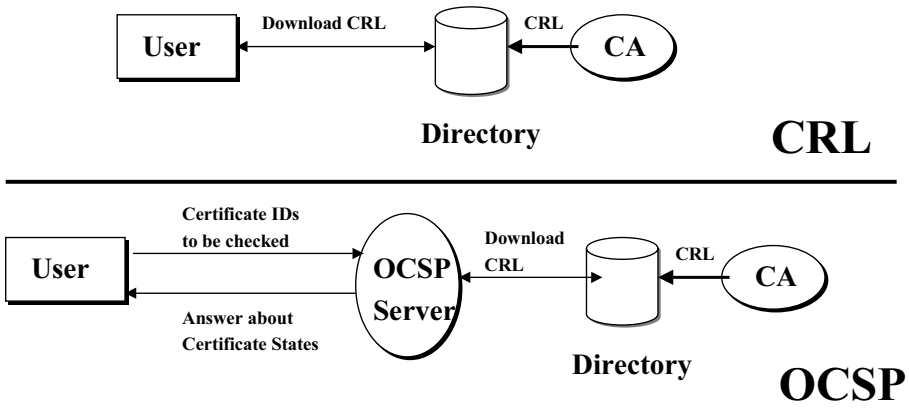


Certificate Revocation List

Revoked Certificates remain in CRL until they expire

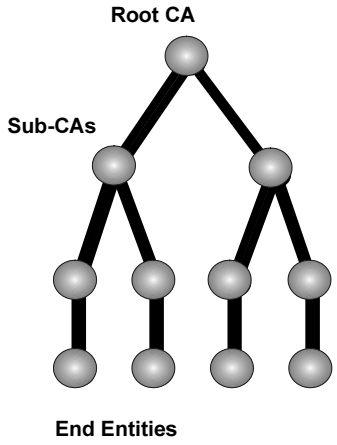


CRL vs OCSP Server



X509 PKI Trust by Hierarchies and Cross Certification

Simple Certificate Hierarchy

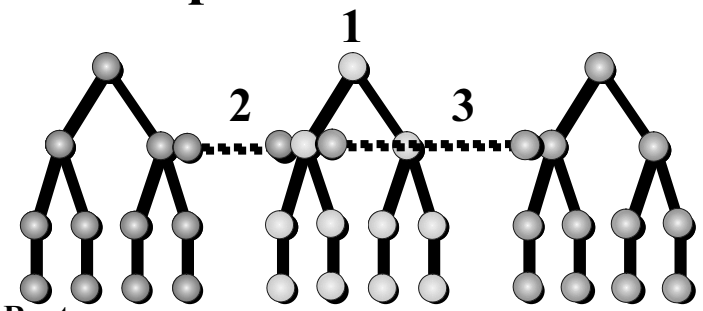


Each entity has its own certificate (and may have more than one). The root CA's certificate is self signed and each sub-CA is signed by its parent CA.

Each CA may also issue CRLs. In particular the lowest level CAs issue CRLs frequently.

End entities need to "find" a certificate path to a CA that they trust.

Cross-Certification and Multiple Hierarchies



- Multiple Roots
- Simple cross-certificate
- Complex cross-certificate

X509 PKI
Approach to Trust : Problems

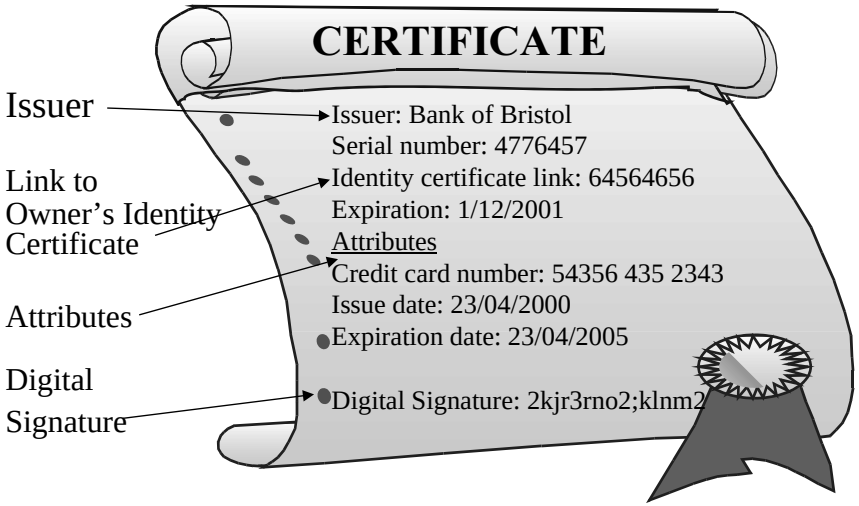
Things are getting more and more complex when Hierarchies and Cross-Certifications are used

Identity is Not Enough: Attribute Certificates

IETF (PKIX WG) is also defining standards for Attribute Certificates (ACs):

- **Visa Card (Attribute) vs. Passport (Identity)**
- **Attribute Certificates specify Attributes associated to an Identity**
- **Attribute Certificates don't contain a Public key but a reference to an Identity Certificate**

Attribute Certificate



Policies and Policy Management

What is Policy

Policy is about the *constraints* and *preferences* on the state, or the state transition, of a system.

It is a guide on the way to achieving the overall objective which itself is also represented by a desirable system state.

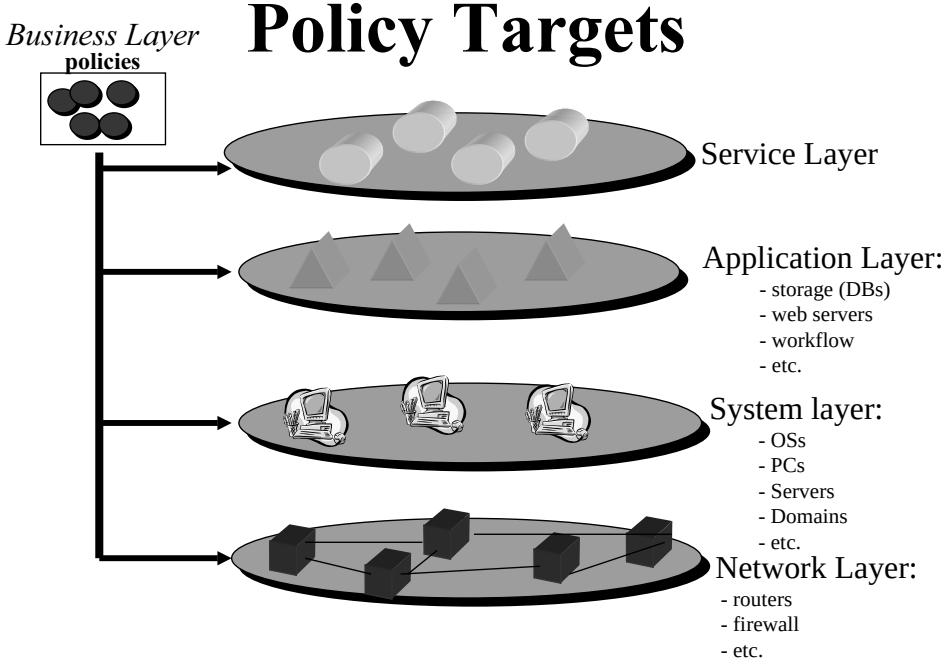
Examples of Policies

- **The IT infrastructure of this company must be secure**
- **Only authorised people can access company confidential documents**
- **Each employee must renew their password every 3 months**
- **The network throughput must at least be 2 Mbits/sec**

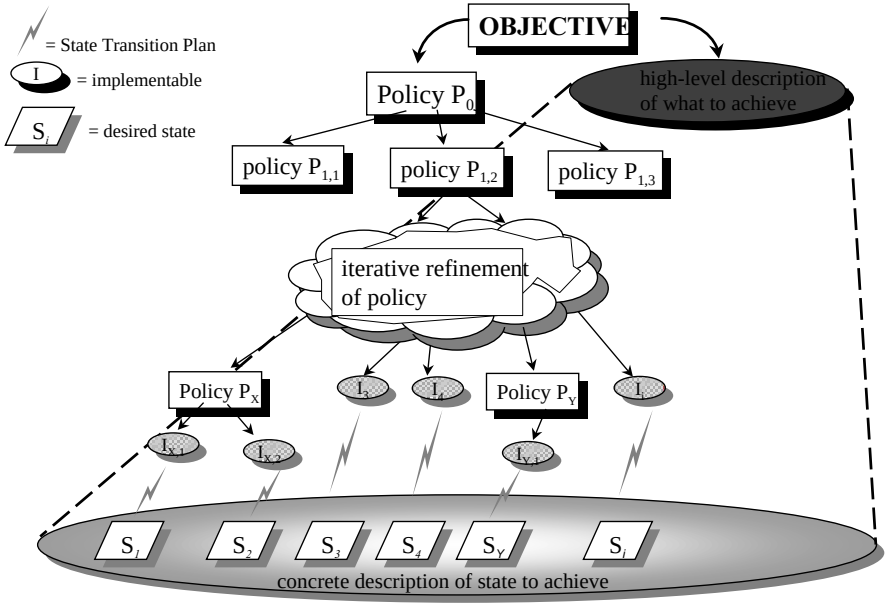
Policies

- **Focus on multiple "IT infrastructure" levels**
- **Can be very abstract: need for refinement**
- **Can be programmatically enforceable or not (focus on the former ones)**

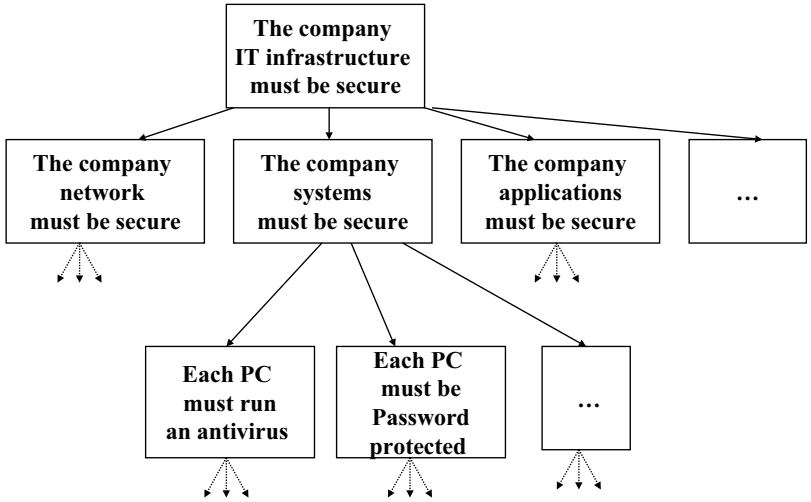
Policy Targets



Policy Refinement



Policy Refinement: Example



Work on Policies

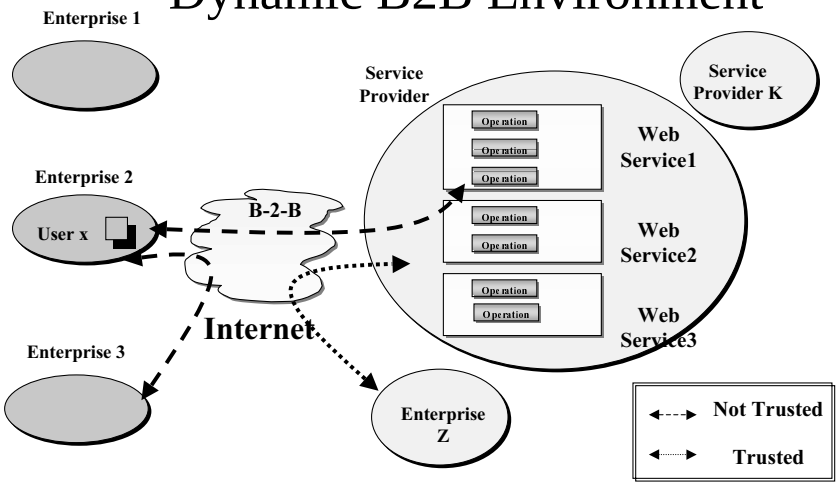
- Imperial College London - Morris Sloman, Emil Lupu
  http://www.doc.ic.ac.uk/~mss/MSSPubs.html
  Policies for Distributed Systems
  (Authorization, Obligation Policies …)
- Other people: Masullo M.: Policy Management
  Wies, R. – Neumair, R.: Application of policies
  Wies: policy specification and transformation
  Heiler, K.: Policy driven Configuration Mnagement
  …
- IETF working groups: www.ietf.org
  policies at the networking level
- …

PART 2

PASTELS

Providing Solutions and Infrastructure to underpin Trust in B2B E-Commerce

Context
Dynamic B2B Environment

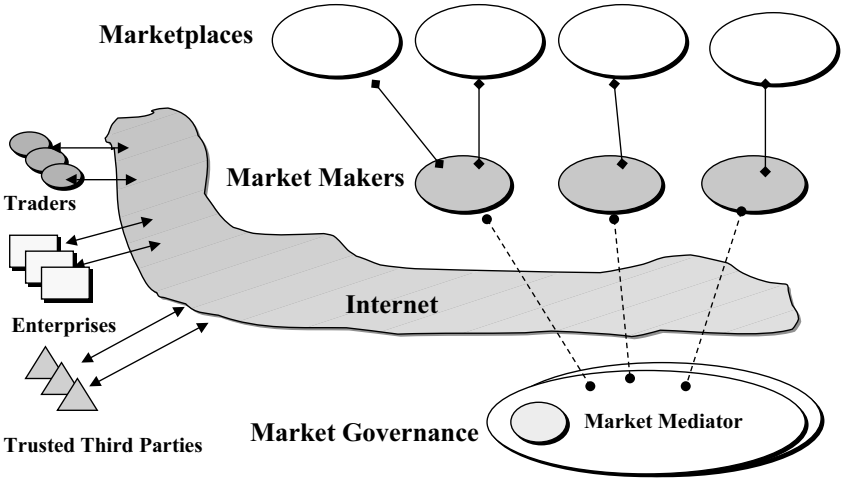


PASTELS Project: Focus

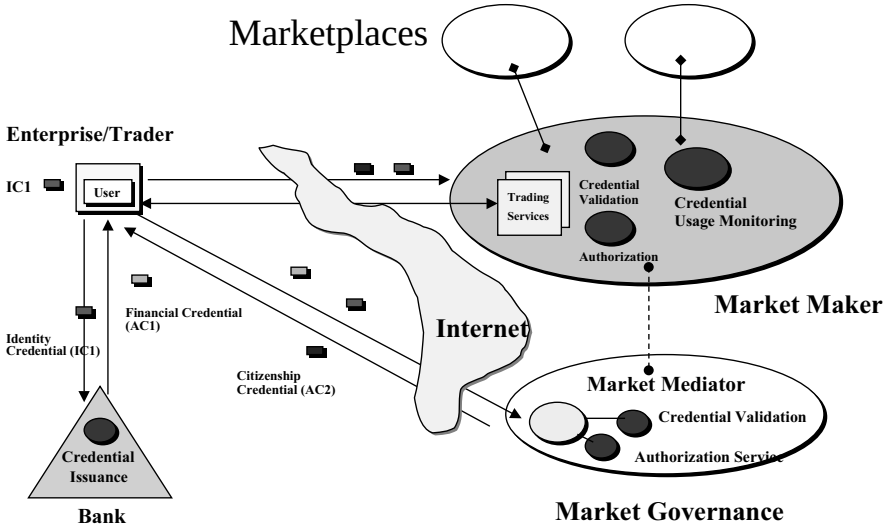
Trust and Trust Management is potentially a huge area. Focus on:

- Framework to deal with Digital Credentials
  - End to End Credential Exchange
  - Solutions for Client and Server Side
- Integration of Digital Credentials with Authorization at the E-Service level

E-Market Context



Simplified E-Market Scenario



Example: Market Maker

- The Market Maker Administrator has to decide which Credential Issuers is going to Trust
- The Administrator has to decide how to deal with Credentials Content:
  - Attribute Semantic
  - Defining policies on which Credential Attributes must be accepted
  - Map to Local Interpretation

Example: Market Maker

- The Administrator has to define Vetting Policies to allow/deny an Enterprise to enter in a Marketplace:
  - for example based on Credentials content: Credit Limit, Ranking, Issuer of Credentials, etc.

"A User with a Credit Limit greater that $100000 and Certified by Issuers "Issuer ABC" can trade in the Marketplace XYZ, during business hours"

Example: Market Maker

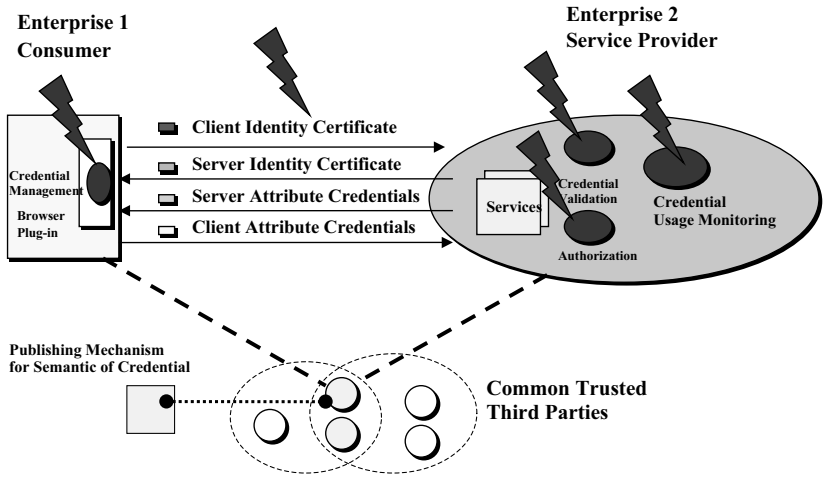
- The Administrator has to define Authorization Policies for Marketplace Services:
  - for example based on Credentials content: Credit Limit, Citizenship Validity, Ranking, etc.

"A User can bid if they have a valid Citizenship, the bid is less than the associated Credit Limit and greater than the current price"

PASTELS Infrastructure & Solutions

PASTELS: Areas of Interest

Infrastructure and solutions to underpin Trust in B2B:



PASTELS

- Models: Credentials, User and Roles, Policies, Services
- Runtime Validation and Authorization Components

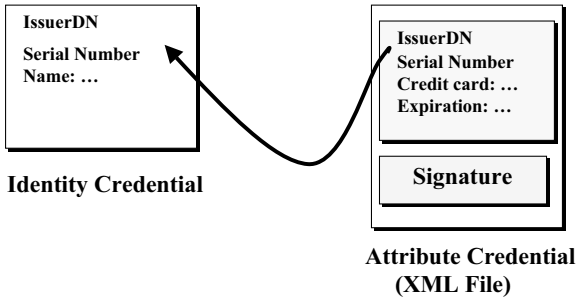
PASTELS: Model of Digital Credentials

Digital Credentials

- Identity Certificates
  - real life: your passport, identity card, etc.
- Attribute Credentials
  - real life: your driving license, bank statement, your credit card, etc.

PASTELS: Attribute Credential Based on Digital Signed XML

- Attribute Credentials are associated to Identity Certificates by using its Issuer DN and Serial Number:



PASTELS:Attribute Credentials

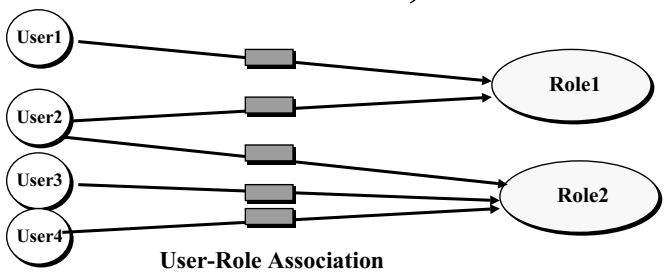
- Attribute Credentials carry "Attributes" with no Explicit Authorization purposes
- Authorization Policies at Service Level are defined within the Enterprise that provides Services.
- An Attribute defined in a Credential becomes relevant for Authorization purposes in the context of an Authorization Policy

PASTELS:

Model of

Users and Roles

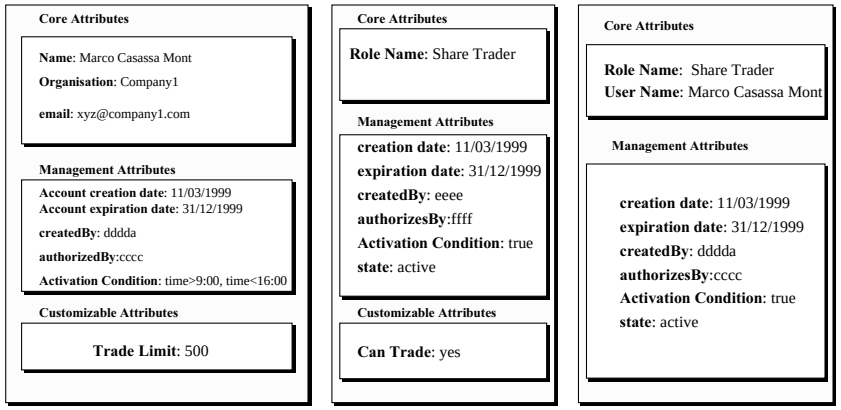
Model - Users, Roles



User, Role, User-Role Association Models based on Attributes:

- **Core Attributes**
- **Management Attributes**
- **Customisable Attributes**

Model - Users, Roles



User: XYZ **Role: Share Trader** **User-Role Association**

PASTELS:

Model of

Authorization Policies

Policy

- Logical expression containing constraints on user profile, user's roles, system information, service parameters, credential content, nature of credentials, external information
- Java like policy language. No PROLOG.
- Interpreted at runtime by the Authorization Engine (policy internal representation)
- Policies can be used to describe constraints of different nature: Validation, Credential Content Management, Authorization

Policy Example

Authorization Policy:

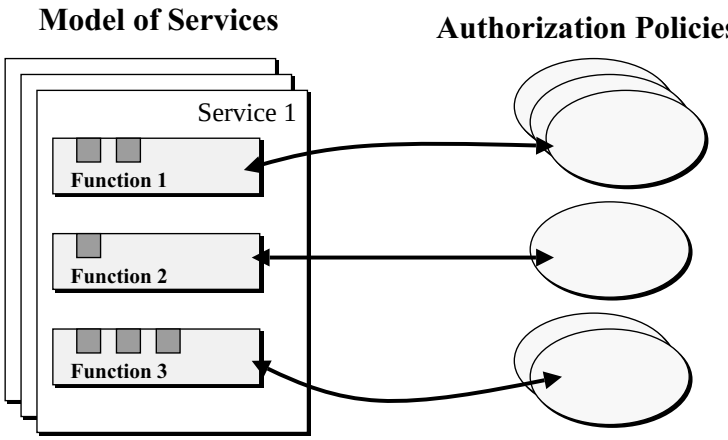
"A User can bid if they have a valid Citizenship Credential, the bid is less than the associated Credit Limit and greater than the current price"

```
EXISTS
        (ASSIGN(CitizenshipNumber, CONTEXT.CitizenshipNumber))
VERIFY
        ((CitizenshipNumber.value > 0) &&
         (CitizenshipNumber.propertyQualifier == "attributeCredential") &&
          ASSIGN(CitizenshipCredential, CitizenshipNumber.scope) &&
          (CitizenshipCredential.IssuerDN == "CN=The MarketGovernance, …")) &&
(bid.bidValue > 0 ) &&
(bid.bidValue > currentPrice.value ) &&
(bid.bidValue <= CONTEXT.CreditLimit )
```

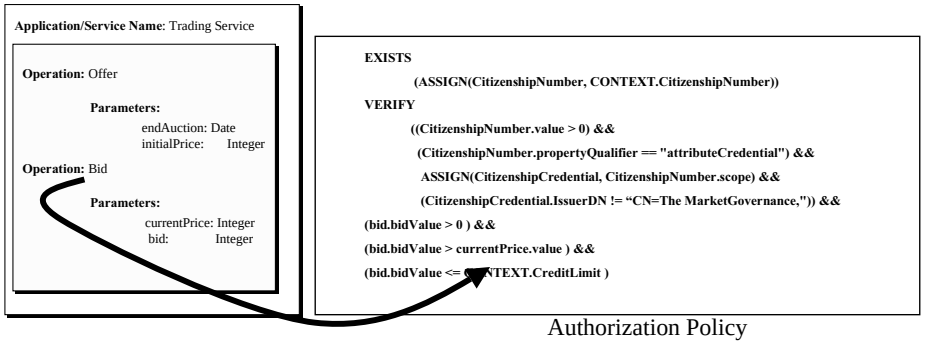
PASTELS

Model of Services

Explicit Service Model



Explicit Service Model



Service Model
(XML based)

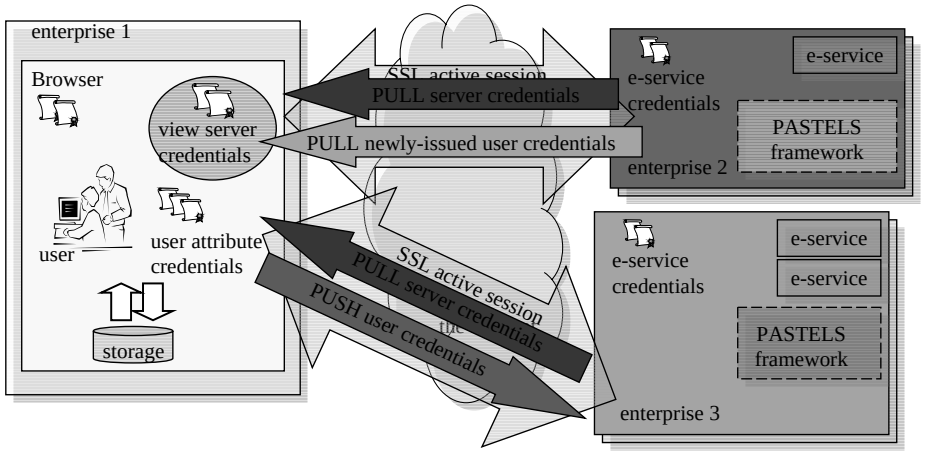
Authorization Policy

PASTELS

Distributed System

Run-time

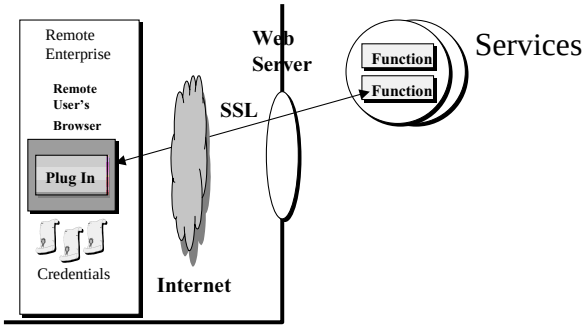
High Level Interaction



PASTELS Framework Runtime Components

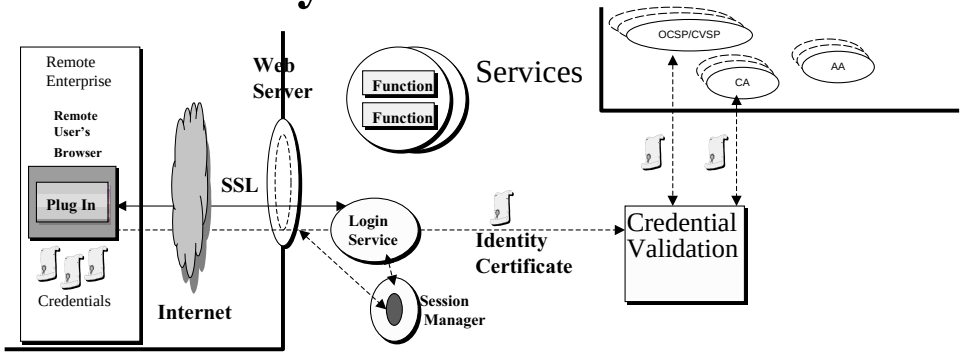
- Login Service: manages login, after basic authentication
- Session Manager: manages user sessions
- Credential Proxy: PUSH/PULL of credentials (browser plug-in)
- Credential Validation Manager: validation of Credentials
- Credential Content Manager: manages credential's content
- User Context Manager: collects user's profile, roles and credentials
- Object Pool Manager: cache for user's profile, roles and credentials
- User Context Gateway: gateway to the Credential Usage Monitoring Sys
- Authorization Server: Policy driven Authorization Server

User's Goal: Access Service



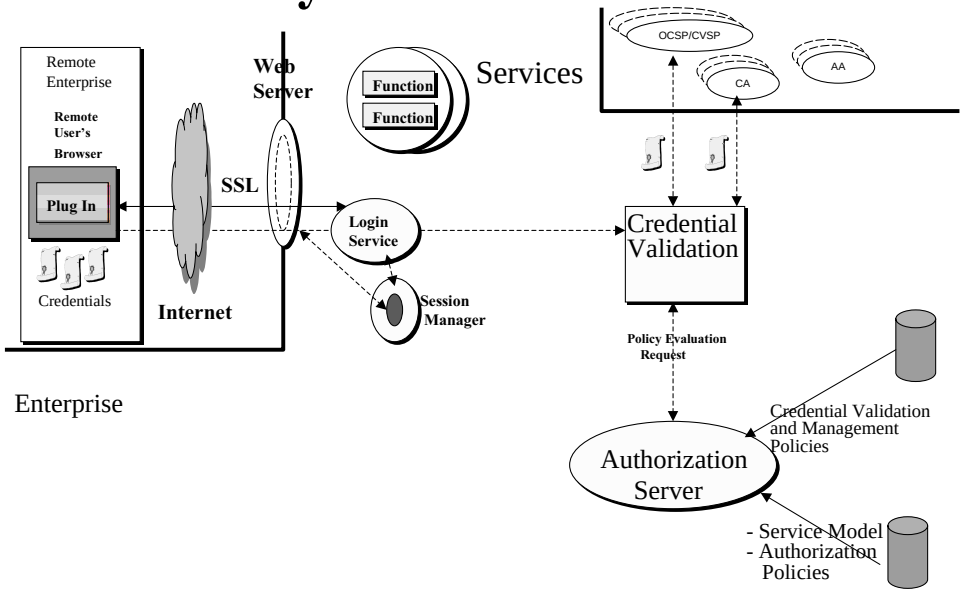
Enterprise

Identity Certificate Validation

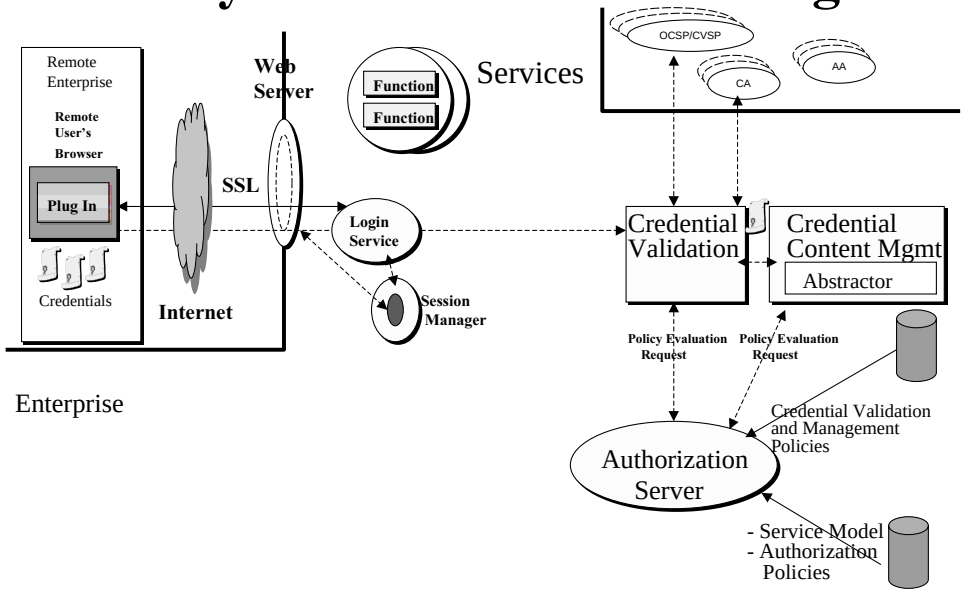


Enterprise

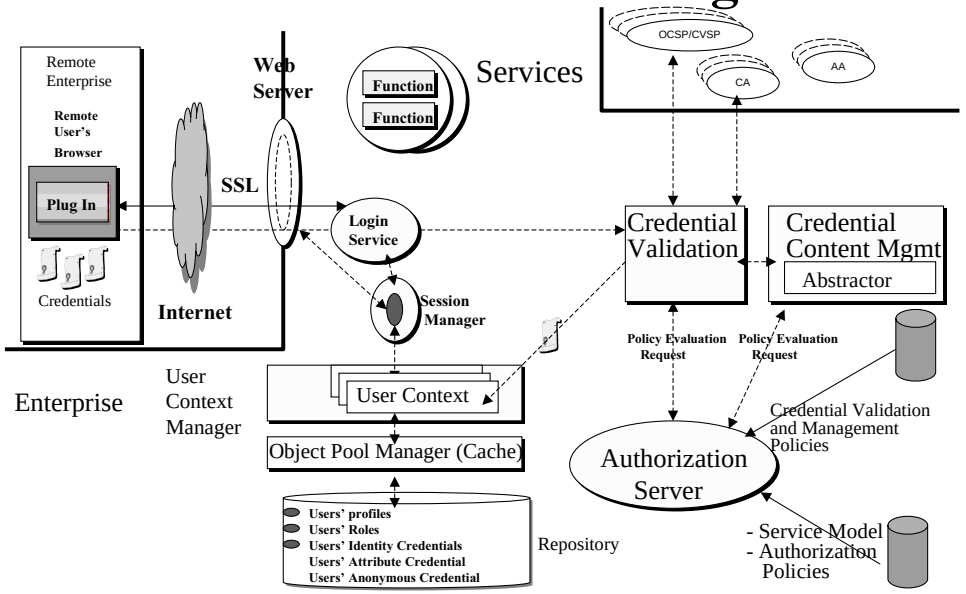
Identity Certificate Validation



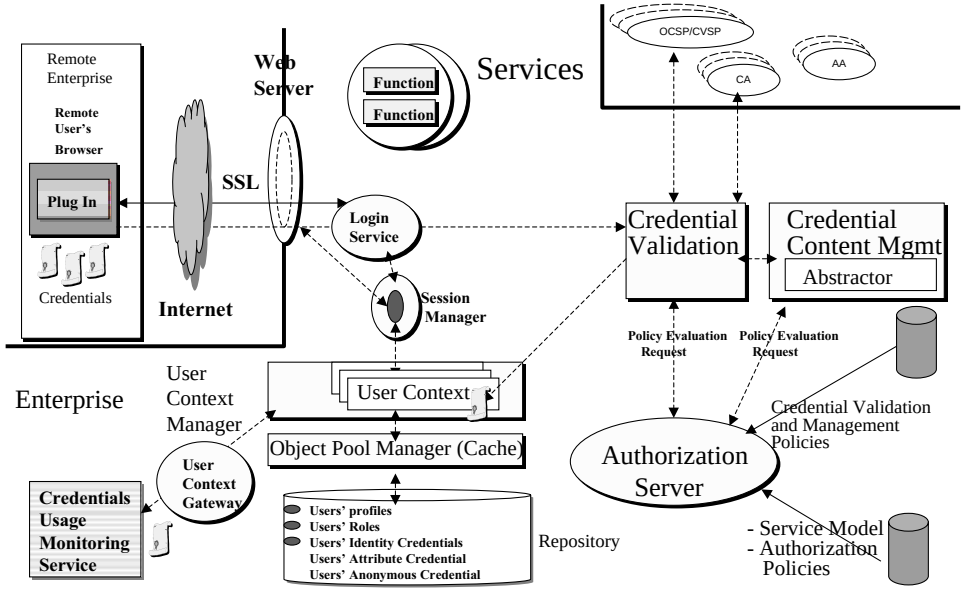
Identity Certificate Content Mgmt



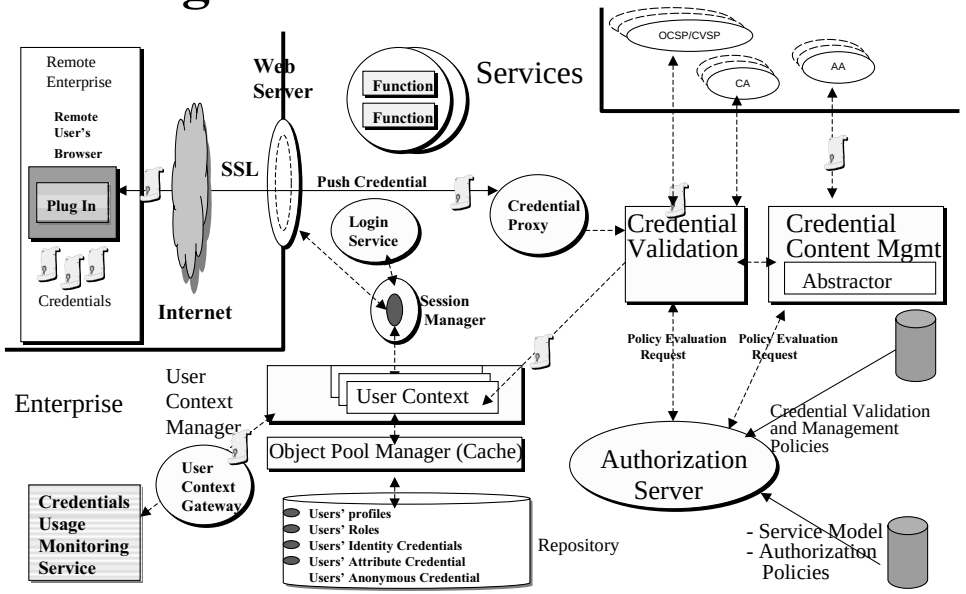
User Context Manager



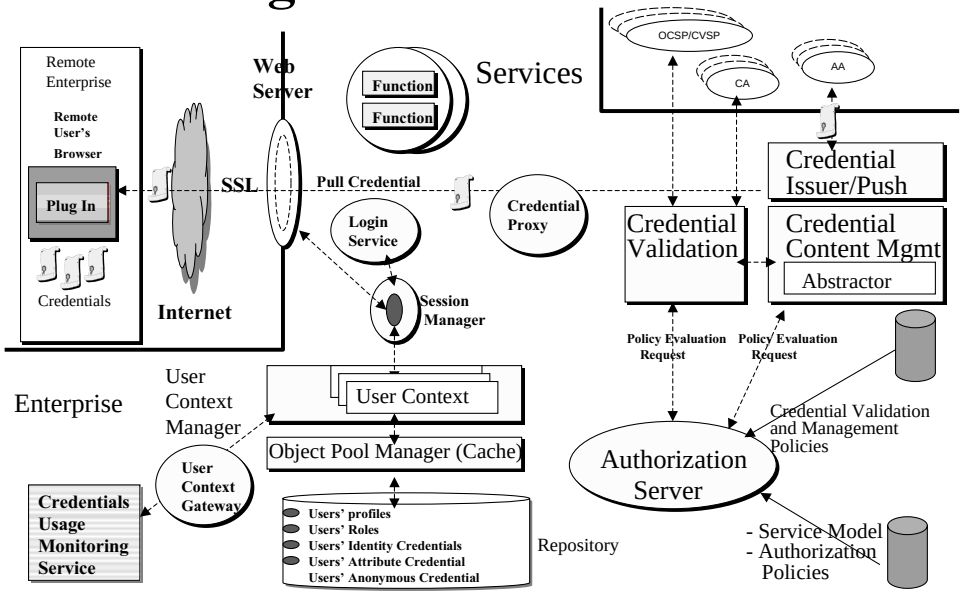
Link to "TrustView"



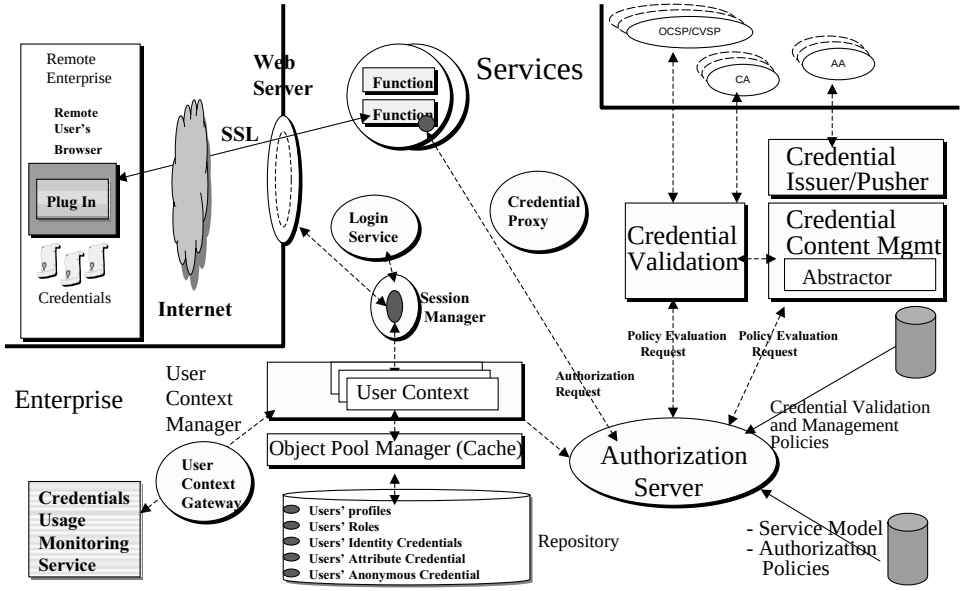
Pushing a User's Attribute Credential



Pulling Attribute Credentials



Authorization at Service Level



Credential Usage Monitoring Service

PASTELS Prototype

- Prototype leverages State of the Art technology:
  - PKI and PKI toolkits (Baltimore UniCERT, J/PKI-Plus)
  - Signed XML (Baltimore X/Secure)
  - SSL with full handshake
  - Web server technology (IIS, JWS)
  - Enterprise Java Beans (EJB)
  - Relational Database (MS SQL Server, MS Access)
  - Object Oriented Database (Cloudscape)

Trust Management Prior Relevant Work

- SPKI (Ellison): Delegation Model
- IETF: X509 RFC, Attribute Certificate RFC
- PolicyMaker (Blaze): Trust Management System
  - Assertions of certificates and policies
  - Policy: key <--> local policy
  - Verify that actions conform to policies and credentials

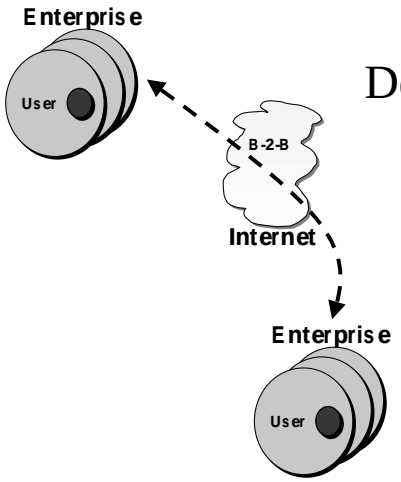
Trust Management Prior Relevant Work

- KeyNote (Blaze): Trust Management System
  - It derives from PolicyMaker
  - Common language for credentials and policies
  - Policy: action permitted by the holder of a public key
- REFEREE (LaMacchia): Trust Management System
  - Environment to evaluate compliance with policies
  - Self-regulated by policies
  - Based on Credentials

PART 3

Moving Towards The Future …

Trust Services

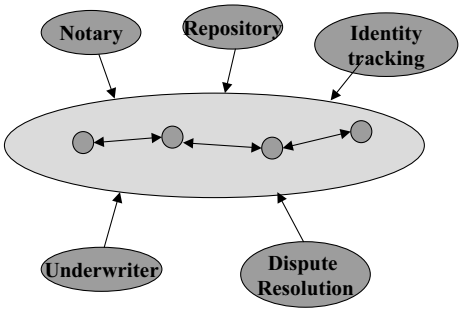


Dealing with things when they go wrong

…

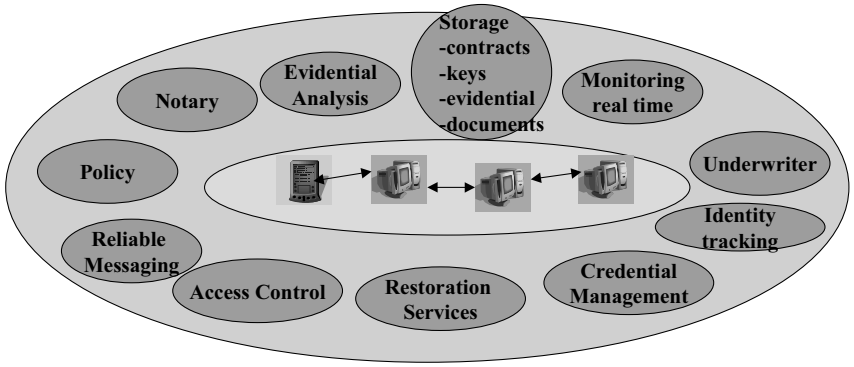
Trust Services as a Safety Net For E-Commerce

Moving Trust to the E-World



Trust Services exist in the physical world. In the E-World the wheels still need greasing. However, the interactions are different.

Greasing the wheels of E-Commerce



Trust Service Eco-system

Trust Services Research Problems …

- Integrity
- Authenticity
- Confidentiality
- Non-Repudiation

- Longevity
- Survivability
- Accountability
- Simplicity